

Sebastian High-Speed Internet Disclosures - Pricing and Network Management Practices

Pricing: Prices and speeds for Sebastian’s basic internet offerings are provided on this website at: sebastiancorp.com/residential/stay-connected. Sebastian may offer additional services and prices in your area. Please contact our business office for possible alternatives. Sebastian’s commercial terms of use, payment, termination policies and privacy policies are available on this site at sebastiancorp.com/customer-service/terms-conditions/.

As required by the “Restoring Internet Freedom” order issued by the Federal Communications Commission, Sebastian discloses its network management practices as follows:

Blocking: Sebastian does not block or prevent end-user access to lawful content, applications, services, or non-harmful devices. In the event of a Distributed Denial of Service (DDoS) attack against a specific customer, if the attack is severe enough to degrade overall network performance, Sebastian will attempt to block the incoming malicious traffic. If this is not technically feasible and there is no other way to stop the attack, Sebastian may temporarily take the targeted endpoint offline. If so, Sebastian will notify the customer of the situation and restore service as quickly as possible.

Throttling: Sebastian does not “throttle” Internet traffic. “Throttling” is defined as degrading or impairing access to lawful Internet traffic on the basis of content, application, service, user, or use of a non-harmful device.

Affiliated Prioritization: Sebastian does not engage in affiliated prioritization. Affiliated prioritization is the practice of directly or indirectly favoring some traffic over other traffic to benefit an affiliate.

Paid Prioritization: Sebastian does not engage in paid prioritization. Paid prioritization is defined as directly or indirectly favoring some traffic over other traffic in exchange for consideration, monetary or otherwise.

Congestion Management: Sebastian does not employ congestion management practices such as usage limits or restrictions during peak activity periods. Sebastian will take steps to mitigate congestion caused by a DDoS attack, as described above.

Application-Specific Behavior: Sebastian does not apply application-specific network management practices. This includes blocking or rate-controlling specific protocols or protocol ports, modifying protocol fields in ways not prescribed by the protocol standard, or otherwise inhibiting or favoring certain applications or classes of applications.

Device Attachment: Sebastian provides a modem for use with its services. This modem provides the ability for Sebastian to remotely provision services and verify signals to the router. Customer provided modem equipment may operate, but will hamper Sebastian’s ability to operate the network effectively. Sebastian is not responsible for connection issues if the modem has been replaced or modified.